REMARKS

The present application has been reviewed in light of the Office Action dated December 23, 2008. Claims 1-7, 10, and 11 are presented for examination, of which Claims 1, 7, 10, and 11 are independent form. Claim 11 has been added to provide Applicant with a more complete scope of protection. Claims 1, 2, 3, 7, and 10 have been amended to define aspects of Applicant's invention more clearly. Support for the claim amendments may be found, for example, in FIG. 14 and at page 22, line 23, to page 23, line 23. Favorable reconsideration is requested.

The Office Action states that Claims 1, 6, 7, and 10 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,938,154 (*Berson et al.*) in view of U.S. Patent Application Publication No. 2003/0043416 (*Rublee et al.*) and U.S. Patent Application Publication No. 2002/0042880 (*Endoh*); that Claim 2 is rejected under 35 U.S.C. § 103(a) as being unpatentable over *Berson et al.* in view of *Rublee et al.* and *Endoh*, and further in view of U.S. Patent Application Publication No. 2003/0163730 (*Roskind et al.*) and U.S. Patent No. 7,117,493 (*Matasushima*); that Claims 3 and 4 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Berson et al.* in view of *Rublee et al.* and *Endoh*, and further in view of *Matasushima* and U.S. Patent No. 7,158,657 (*Okazaki et al.*); and that Claim 5 is rejected under 35 U.S.C. § 103(a) as being unpatentable over *Berson et al.* in view of *Rublee et al.* and *Endoh*, and furhter in view of *Matasushima* and *Okazaki et al.* and *Roskind et al.* For at least the reasons presented below, Applicant submits that independent Claims 1, 7, 10, and 11, together with the claims dependent therefrom, are patentably distinct from the cited prior art.

The aspect of the present invention set forth in Claim 1 is directed to a remote

operation method of an information processing apparatus connected to an authentication apparatus and an image processing apparatus via a network. The method includes: (1) an accessing step of accessing the image processing apparatus, (2) a reception step of receiving from the image processing apparatus data for specifying the authentication apparatus, which authenticates an operation level of a remote operation, as a response to the accessing in the accessing step, (3) a request step of issuing a request for the authentication process to the authentication apparatus based on the data received in the reception step in a case where an instruction to operate remotely the image processing apparatus is input by a user, wherein the authentication process is to authenticate an operation level of the remote operation performed by the information processing apparatus, and (4) a remote operation step of, upon remotely operating the image processing apparatus, performing an executable kind of remote operation specified by the operation level authenticated in the authentication process.

Notable features of Claim 1 are that the request for the authentication process is issued to the authentication apparatus based on the data received, in a case where the instruction to operate remotely the image processing apparatus is input by the user, in which the authentication process is to authenticate the operation level of the remote operation performed by the information processing apparatus. Upon remotely operating the image processing apparatus, an executable kind of remote operation is performed, in which the executable kind of remote operation is specified by the operation level authenticated in the authentication process. By virtue of these features, the image processing apparatus need not be enabled to authenticate the operation level of the remote operation performed by the host computer; instead the image processing apparatus simply provides the host apparatus with data specifying an authentication

apparatus, for example.[1/]

Berson et al. relates to identification, management, and operation of network devices (*see* col. 1, lines 8-11). *Berson et al.* discusses a process for secure operation of a network device, such as a printer, a copier, a scanner, or a facsimile machine (*see* FIG. 3). As understood by Applicant, *Berson et al.* does not teach or suggest an authentication process to authenticate an operation level of a remote operation performed by an information processing apparatus, nor does *Berson et al.* teach performing an executable remote operation specified by the authenticated operation level.

Rublee et al. relates to a system for scanning hard-copy images to electronic mail addresses (*see* paragraph 1). *Rublee et al.* discusses that a scanner sends a host name of an authentication server to a domain name server, which responds by sending a corresponding address of the authentication server to the scanner (*see* page 3, paragraph 25). As understood by Applicant, *Rublee et al.* does not teach or suggest an authentication process to authenticate an operation level of a remote operation performed by an information processing apparatus, nor does *Rublee et al.* teach performing an executable remote operation specified by the authenticated operation level.

Endoh relates to managing the use of a peripheral device such as a printer, a scanner, a copier, and a facsimile (*see* paragraph 2). *Endoh* discusses that a peripheral device can perform user authentication by displaying a dialog on a console and processing user information input via the console (*see* paragraph 5). *Endoh* also discusses that a peripheral device can

---

1/ Any examples presented herein are intended for illustrative purposes and are not to be construed to limit the scope of the claims.

perform a process each time the device receives a job command (*see* paragraph 99). When a job command is received by the device, the command and its parameter are analyzed to determine whether the command is an attribute setting command and whether an attribute of the command can be interpreted by the device (*see* paragraph 99). If the attribute can be interpreted, a specified attribute name and attribute value are stored as job data (*see* paragraph 100). If the attribute cannot be interpreted, the device informs a sender of the command that the attribute could not be set (*see* paragraph 100).

The device also determines whether the received command is a job data transmission command and, if so, received job data following the command is stored (*see* paragraph 101). If the received command is not the job data transmission command, the device determines whether the received command is a job submitting termination notice command and, if so, processing of job data is started (*see* paragraph 102). If the received command is not the job submitting termination notice command, the received command is another command, and a corresponding process is performed (*see* paragraph 102).

In addition, *Endoh* discusses that a data structure of a job held in the device includes an attribute list, which includes pairs of attributes names and corresponding attribute values, and job data, which includes data to be a processing target of the job (*see* paragraph 103). The data structure of the job may include data representing that the job is a printing job, data representing that a job starting mode is pending, data representing that a user management mode is "Join Security Domain" indicating that an access ticket is used as user information for the job, data representing an attribute for which a user ID is set if a user management mode is "User ID" or "User ID and Password," data representing an attribute for which a password is set if the user

management mode is "Password" or "User ID and Password," data representing an attribute for which the access ticket is set if the user management mode is "Join Security Domain" (*see* paragraph 104).

Endoh also discusses a procedure for a job data held in the peripheral device, wherein attribute information (*e.g.,* a current user management mode) is obtained and processed to determine whether the attribute information is "No User Management" (*see* paragraph 105). If the attribute information is "No User Management," processing of certain job attributes is performed, processing of job data is performed based on these attributes, and job processing results are stored (*see* paragraph 106). If the attribute information is "Password," a stored password is compared to corresponding attribute information and, only if they match, does precessing of the job continue (*see* paragraph 107). If the attribute information is "User ID," a stored user ID is compared to corresponding attribute information and, only if they match, does precessing of the job continue (*see* paragraph 108). If the attribute information is "User ID and Password" a stored user ID value and a stored password are compared to corresponding attribute information and, only if they match, does precessing of the job continue (*see* paragraph 109).

Endoh, however, does not teach or suggest an authentication process to authenticate an operation level of a remote operation performed by an information processing apparatus, nor does *Endoh* teach performing an executable remote operation specified by the authenticated operation level.

In summary, Applicant submits that a combination of *Berson et al.*, *Rublee et al.*, and *Endoh*, assuming such combination would even be permissible, would fail to teach or suggest a method that includes "a request step of issuing a request for the authentication process to the

authentication apparatus based on the data received in the reception step in a case where an instruction to operate remotely the image processing apparatus is input by a user, wherein the authentication process is to authenticate an operation level of the remote operation performed by the information processing apparatus," and "a remote operation step of, upon remotely operating the image processing apparatus, performing an executable kind of remote operation specified by the operation level authenticated in the authentication process," as recited in Claim 1. Accordingly, Applicant submits that Claim 1 is patentable over *Berson et al.*, *Rublee et al.*, and *Endoh*, and respectfully requests withdrawal of the rejection under 35 U.S.C. § 103(a).

Independent Claims 7, 10, and 11 include features similar to those of Claim 1 and are believed to be patentable for at least the reasons discussed above. The other rejected claims in the present application depend from Claim 1 and are submitted to be patentable for at least the same reasons. Because each dependent claim also is deemed to define an additional aspect of the invention, individual reconsideration of the patentability of each claim on its own merits is respectfully requested.

No petition to extend the time for response to the Office Action is deemed necessary for this Amendment. If, however, such a petition is required to make this Amendment timely filed, then this paper should be considered such a petition and the Commissioner is authorized to charge the requisite petition fee to Deposit Account 06-1205.

In view of the foregoing amendments and remarks, Applicant respectfully requests favorable consideration and an early passage to issue of the present application.

Applicant's undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our below listed address.

Respectfully submitted,

/Lock See Yu-Jahnes/

_____

Lock See Yu-Jahnes
Attorney for Applicant
Registration No. 38,667

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

FCHS_WS 2768690v1